Chapter 2

Security and System Management

2.1 Security

2.2 Customer Service Center

Contents

Chapter 2: Security and System Management

2.1 Security 2–1
2.1.1 Personnel Security 2–1
2.1.1.1 User Organization Access 2–2
2.1.1.2 User ID for ED Users 2–3
2.1.1.3 User ID for Non-ED Users 2–4
2.1.1.4 Passwords 2–5
2.1.1.4.1 Replacing Your Temporary Password 2–5
2.1.1.4.2 Changing Your Password 2–6
2.1.1.4.3 Restrictions 2–6
2.1.1.4.4 Requesting a Password Reset 2–6
2.1.2 System Security 2–6
2.1.2.1 Application Protection Levels 2–7
2.1.3 Physical Security 2–7
2.1.3.1 Computer Facilities 2–7
2.1.3.2 Magnetic Media 2–8
2.1.3.3 Printed Matter 2–8
2.2 Customer Service Center 2–8
2.2.1 Responsibilities and Services 2–9
2.2.2 Operating Procedures 2–9
2.2.3 Problem Reporting 2–10

Figures

Figure 2–1, Notice of Criminal Liability 2–1
Figure 2–2, NSLDS Functional Groups 2–7

2.1 Security

The following section contains *important* security information. Please read it carefully. Each NSLDS user must participate in system security on these three levels:

1. Personnel Security
2. System Security
3. Physical Security

As an authorized user of NSLDS, you are *personally liable* for any unauthorized disclosure of NSLDS data subject to the Privacy Act of 1974, as amended, or for failure to adhere to NSLDS standards and procedures. An abstract of the Privacy Act is presented in Figure 2–1. This statement is a reminder of the liability that accompanies access to, and use of, the system. It is also a verbatim copy of the statement signed by you, other employees, and contract personnel when applying for a security clearance with ED and by users applying for access to NSLDS.

Notice of Criminal Liability Under the Privacy Act

The information provided to me by the Department of Education is protected by the Privacy Act of 1974, as amended. The protection of this information, once entrusted to me, becomes my responsibility. Therefore, I agree to protect the privacy of all information that has been provided to me as an agent of the Department. I understand that the criminal penalties identified below may be enforced if I violate the requirements of the Privacy Act.

5 U.S.C. § 552a, as amended,

(*i*)(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

I certify that I have read and understand the criminal penalties of the Privacy Act, as stated above, and that I agree to comply with the government's requirements for the protection of any information covered by the Privacy Act.

Source: The Privacy Act of 1974 (as amended)

Figure 2–1, Notice of Criminal Liability

2.1.1 Personnel Security

The NSLDS database contains information about private citizens that is subject to the provisions of Public Law (PL) 93-579, the Privacy Act of 1974. NSLDS is designed to protect data from

both intentional and inadvertent disclosure or destruction. Output from NSLDS computers or terminals, printed reports, magnetic media, and downloaded files, may contain data that is subject to the Privacy Act and must be protected by the organization and the individual user.

To use NSLDS, an individual must be an approved member of an organization authorized to access the system. The individual must also hold a valid user ID and password. The following subsections define the process for becoming an authorized NSLDS user.

NOTE: Students who use the student access site must have a valid PIN that correlates to the first two letters of his or her last name and birth date.

2.1.1.1 Organization Application Process for NSLDS Access

For an organization to access NSLDS, it must execute a formal agreement with the NSLDS Division of ED. Each organization desiring access to the system must submit the NSLDS Privacy Act Acknowledgment Statement (Form SEC004) for approval.

The application process consists of the following steps:

1. You or someone at your organization must obtain a Form SEC004 from the Customer Service Center (CSC) by calling 1-800-999-8219. Detailed instructions to assist you in completing the form are provided on the form's reverse side.

2. Complete the form, sign block 2a on Form SEC004, and submit the form for ED approval to this address:

   United States Department of Education
   National Student Loan Data System
   1250 Maryland Ave., SW
   Portals Bldg. Room 602
   Washington, DC 20202
   Attn: NSLDS Division ACSO

3. The NSLDS Division Application Computer Security Officer (ACSO) reviews the Organization Participation Agreement Form and the Privacy Act Statement Form for ED and, after approval, forwards the original and Form SEC004 to the Virtual Data Center (VDC) contractor.

4. The VDC contractor assigns the RACF security and forwards the forms to the CSC.

5. The CSC associates the user to the appropriate function groups indicated by the VDC contractor. The CSC also updates the names and addresses in CICS.

6. The CSC assigns a group ID to the organization to control levels of access to the system and assigns a billing group ID for accounting purposes. The system generates a letter that notifies the organization that it may access NSLDS and apply for individual user IDs.

2.1.1.2 User ID for ED Users

An NSLDS user identification (user ID) is a unique, multi-character description the system uses to recognize an authorized user. To obtain a user ID, you must submit an NSLDS User Participation Request Form (SEC003) through your supervisor to the NSLDS Division ACSO for approval.

To acquire an NSLDS user ID, an ED user must complete the following steps:

1. Obtain an official copy of the NSLDS User Participation Request Form (SEC003) from your supervisor or the NSLDS Division ACSO. *Detailed instructions are provided on the reverse side of each form to assist you in completing the process.*

2. Fill in blocks 1, 2, and 3; then submit Form SEC003 to your supervisor for review and approval. Your supervisor completes blocks 4 and 5 and forwards Form SEC003 to your organization's Computer Security Office (CSO).

   The CSO completes block 6 and forwards Form SEC003 to the NSLDS Division ACSO for approval, at this address:

   United States Department of Education
   National Student Loan Data System
   1250 Maryland Ave., SW
   Portals Bldg. Suite 600B
   Washington, DC 20202
   Attn: NSLDS Division ACSO

   The NSLDS Division ACSO authorizes your request by signing block 7 and forwarding the original Form SEC003 to the CSC.

3. Your assigned user ID and initial password are mailed to the NSLDS Division ACSO for distribution. *If you are attending the NSLDS Training Course, your notification will be delivered at the end of the course, along with an initial password, and you will be assisted in your initial logon. In this event, you may omit Step 4.*

4. After receiving notification from the NSLDS Division ACSO, log on to NSLDS using the initial password, and follow the steps in Section 2.1.1.4 for selecting a new private password. For first-time logon support, call the CSC for help.

2.1.1.3 User ID for Non-ED Users

Non-ED user organizations include other Government agencies and the following private organizations: GAs, schools, lenders, and servicers.

A user ID is a unique, multi-character description the system uses to recognize an authorized user. To obtain an NSLDS user ID, you must process a formal request through your supervisor to ED for approval. You must also complete an NSLDS Privacy Act Acknowledgment Statement (Form SEC004) and include it with your application.

A non-ED user must complete the current Student Aid Internet Gateway (SAIG) enrollment document. The SAIG enrollment document can be submitted these two ways:

- Go to sfawebenroll.ed.gov/T4Enroll/index.htm. Follow the directions on this web site to complete the SAIG enrollment document and submit it online.

- Download the latest SAIG enrollment document at www.ifap.ed.gov under Dear Partner (Colleague) letter number GEN-99-34. After reading and carefully completing the form, send by U.S. mail to:

  Title IV WAN Customer Service
  P.O. Box 30
  Iowa City, IA 52244

If you have any questions concerning SAIG enrollment using either method, please call Title IV WAN customer service at 1-800-615-1189.

After receiving your completed SAIG enrollment document, Title IV WAN assigns a TG number (Title IV WAN mailbox name) and notifies you by letter. Title IV WAN also sends your enrollment information to NSLDS for user ID assignment.

NSLDS assigns your User ID and sends a letter with your user ID. Another letter follows with your temporary initial password to log on to NSLDS.

When you receive notification from NSLDS, use the new user ID and initial password to log on to NSLDS through the Title IV WAN. Follow the directions in Section 2.1.1.4, Passwords, to select a new, private password. If you need help with your initial logon, call the NSLDS CSC at 1-800-999-8219.

2.1.1.4 Passwords

Passwords follow established conventions and security rules. Each password must:

- Be six to eight characters in length
- Contain at least one alpha and one numeric character
- Change at least once each 120 calendar days to remain active

The NSLDS CSC issues you an initial logon password, which you are responsible for changing and protecting. Avoid using familiar family names, initials, and words. The best passwords use a combination of letters and numerals eight characters in length.

Passwords should NEVER be:

- Revealed to other people
- Written down
- Included as a part of an automatic logon sequence on any PC-based or memory-equipped terminal or system

If you forget your password, contact the NSLDS CSC and request that an authorized NSLDS Security Administrator reset your password.

You must update your password every 120 days. If you do not update your password before the 120th day, it will expire and you will be unable to access NSLDS. If this occurs, contact the NSLDS CSC to request that your password be reset. Also, if you exceed the unsuccessful logon limit of three consecutive failed attempts, you account is locked until the NSLDS CSC resets the password.

2.1.1.4.1 Replacing Your Temporary Password

When you log on to NSLDS successfully for the first time, your temporary initial password expires, and the system prompts you to enter a new password. To enter the new password, follow these steps:

1. Type a new six- to eight-character **Password** in the New Password field. Your password is not displayed as you type, but the cursor advances across the screen.
2. The system prompts you to verify your new password by typing it again in the Confirm Password field.
3. Press **Change Password**.

2.1.1.4.2 Changing Your Password

To change a valid password, follow these steps:

1. From the LogOn Page or Main Menu, select **Change Password**.
2. In the **Current Password** field, type your current password.
3. In the **New Password** field, type your desired password.
4. In the **Confirm Password** field, retype your desired password.
5. Select **Change Password**.

2.1.1.4.3 Restrictions

The NSLDS security system keeps a record of your four most recent passwords and does not allow you to reuse any one of them when your current password expires.

You must update your password every 120 days. If you do not update your password before the 120th day, it will expire and you will be unable to access NSLDS. If this occurs, contact the NSLDS CSC to request that your password be reset. Also, if you exceed the unsuccessful logon limit of three consecutive failed attempts, you account is locked until the NSLDS CSC resets the password.

2.1.1.4.4 Requesting a Password Reset

The NSLDS CSC is responsible for resetting passwords. However, before the NSLDS CSC can reset your password, you must verify your account by providing the NSLDS CSC with confidential information from your NSLDS User Participation Request Form (SEC003). The NSLDS CSC then contacts an NSLDS Security Administrator and authorizes him or her to reset your password. This typically takes an hour or less. When your password is reset, the NSLDS CSC issues you a temporary password. When you log on for the first time with the temporary password, that password expires and you must enter a new password (see Section 2.1.1.4.1).

2.1.2 System Security

NSLDS limits and monitors access to the system to reduce the risk that data might be disclosed or destroyed without authorization. In addition, the NSLDS contractor conducts audits to ensure the effectiveness of system security functions.

2.1.2.1 Application Protection Levels

To access an NSLDS application, you must be a member of a functional group that is authorized to use that application. Some examples of NSLDS functional groups are shown in Figure 2–2.

Group	Application Access
NSLDS User	Generic group used to grant access to menus and initial logon
ED	Generic ED group giving baseline access to all applications
ED Default Management	Access to Default Management applications
ED NSLDS Division	Access to NSLDS Division applications
GA	Generic GA group giving baseline access to applications for GAs
School	Generic school group giving baseline access to applications for schools
Customer Service Center	Access to NSLDS CSC applications
Lender	Generic lender group giving baseline access to applications for lenders

Figure 2–2, NSLDS Functional Groups

Functional groups reflect functional distinctions among users. They are used to provide appropriate access to individuals within pre-defined groups based on their own job functions as well as the function of their organization. Functional groups provide different levels of access to users who are located together or covered by a common level of security. Access limitations for each group are defined when the functional group is established.

Users are assigned to a functional group based on the information provided on the NSLDS User Participation Request Form. When users attempt to execute an application that is not available to their function group, an authorization failure warning message is displayed on their screen.

The system's security design ensures that only the data elements and system capabilities authorized for a given function group are presented in the online menus, screens, queries, and reports that are accessed by members of that group.

If you are unable to access data required for your job, contact the NSLDS CSC. The NSLDS CSC representative will contact your security administrator to determine the proper course of action.

2.1.3 Physical Security

2.1.3.1 Computer Facilities

You must protect your computer hardware from unauthorized access during online NSLDS sessions. You should locate your workstation so that co-workers who are not authorized to access

NSLDS cannot view it during online NSLDS sessions. In addition, you should not leave your workstation unattended during online NSLDS sessions.

2.1.3.2 Magnetic Media

You must clearly mark computer tapes or diskettes containing student loan data to indicate that they contain Privacy Act information, and you must emphasize the penalties for unauthorized disclosure. Tapes or diskettes distributed by the NSLDS CSC are so marked. When you make copies of such tapes or diskettes, you are responsible for ensuring that the correct markings are included. In addition, any computer tape or diskette containing Privacy Act information must be stored in a secure location.

2.1.3.3 Printed Matter

You must clearly mark printed reports containing student loan information to indicate that they contain Privacy Act information, and you must emphasize the penalties for unauthorized disclosure. Reports distributed by the NSLDS CSC are marked in this manner. When you make copies of these reports, you are responsible for ensuring that the correct markings are included. In addition, any printed matter containing Privacy Act information must be stored in a secure location.

2.2 Customer Service Center

From time to time, you may have questions for which you cannot readily find answers. This is why the NSLDS Customer Service Center (CSC) was created. Become familiar with the CSC's responsibilities and services and take advantage of its capabilities. The CSC is operated by the NSLDS contractor and may be contacted as follows:

NSLDS
Customer Service Center

1-800-999-8219

8 a.m. - 8 p.m. Eastern Time

Monday-Friday *

*** except Federal holidays**

2.2.1 Responsibilities and Services

Each authorized NSLDS user may contact the CSC and consult with Customer Service Representatives (CSRs) on a wide variety of related system topics. The CSC is responsible for:

- Coordinating with GAs, schools, and ED users to resolve any transmission problems that affect their ability to obtain data from, or provide data to, NSLDS
- Issuing notices to users informing them of system outages, changes in processing schedules or production programs, and other problems affecting system availability and performance
- Documenting user problems and inquiries
- Helping users to identify their training needs and coordinating with the appropriate training personnel
- Helping users resolve problems with the NSLDS system and software, PC software and hardware, and missing or late reports
- Monitoring and resolving problems with system availability, processing times, priorities, and related performance issues
- Answering security-related questions

2.2.2 Operating Procedures

The CSC is available from 8 a.m. to 8 p.m. Eastern time, Monday through Friday, except federal holidays. The CSC uses an automated control and tracking system to trace user questions or problems and CSC responses. If a caller's question cannot be answered on the telephone with CSC, the caller is told when an answer can be provided. If the caller desires, the CSR can provide a tracking system ticket number for reference. Each problem report has a unique ticket number, which can be used for follow-up inquiries and referrals.

The CSRs are the first point of contact for NSLDS users with problems or questions. CSRs are expected to resolve these types of problems or inquiries during the initial call:

- NSLDS Application Inquiries
- System Availability Questions
- Performance Issues
- Data Transmissions
- Query Inquiries

- PC Problems
- Missing Reports
- Security-Related Issues

Some problems that cannot be resolved by the CSC are transferred to other departments. In this case, the CSC monitors and tracks these problems until closure.

2.2.3 Problem Reporting

If you call the CSC for assistance with a system problem, we ask that you be at your workstation and prepared to give the CSR five important pieces of information:

1. The type of workstation hardware (for example, IBM-compatible) and software (for example, AttachMate EXTRA!) you are using.

2. The exact number and wording of any messages displayed on your screen.

3. The name of the web page you were using when the problem occurred.

4. A description of what happened and what you were doing when the problem occurred.

5. What you tried to do to fix the problem.

This information helps the CSR provide you with a timely response or direct your inquiry to an appropriate specialist for research.